

CLAIM AMENDMENTS

- a 1. (Currently Amended) A method for communicating a session key from a first multicast proxy service node of a secure multicast group to a plurality of other multicast proxy service nodes of the secure multicast group in a communication network, wherein each of the multicast proxy service nodes is capable of establishing multicast communication and serving as a key distribution center, the method comprising the steps of:
- creating and storing [[a]] an original group session key associated with the secure multicast group in a first directory;
- authenticating the first multicast proxy service node with a subset of the multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the secure multicast group, based on the original group session key stored in the first directory;
- receiving a plurality of private keys from the subset of the multicast proxy service nodes;
- receiving a new group session key for the secure multicast group, for use after addition of the first multicast proxy service node, from a local multicast proxy service node that has received the original group session key through periodic replication of the first directory;
- communicating the new group session key ~~private key~~ to the first multicast proxy service node; and
- communicating a message to the subset of the multicast proxy service nodes that causes the subset of the multicast proxy service nodes to update their private keys.

a' 2. (Currently Amended) A method as recited in Claim 1, wherein authenticating the plurality of first multicast proxy service ~~nodes~~ node includes authenticating the plurality of first multicast proxy service ~~nodes~~ node based on a second directory that comprises a directory system agent (DSA) that communicates with one or more of the multicast proxy service nodes and a replication service agent (RSA) that replicates attribute information of the one or more multicast proxy service nodes.

3. (Currently Amended) A method as recited in Claim 1, wherein receiving ~~[[a]]~~ the new group session key includes receiving the new group session key from a node of a second directory that comprises a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes and a replication service agent (RSA) for replicating key information of the one or more multicast proxy service nodes.

4. (Currently Amended) A method as recited in Claim 3, further comprising the step of signaling the replication service agent to carry out replication by storing an updated group session key in a local node of the first directory.

5. (Currently Amended) A method as recited in Claim 1, further comprising distributing ~~[[a]]~~ the original group session key to all nodes by creating and storing the original group session key using a first multicast proxy service node of one domain of the first directory; replicating the first directory; and obtaining the original group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node.

6. (Currently Amended) A method as recited in Claim 1, further comprising distributing ~~[[a]]~~ the new group session key to all nodes by creating and storing the new group session key using a first multicast proxy service node of one domain of the first directory; replicating the first directory; and obtaining the new group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node.

a 7. (Currently Amended) A communication system for ~~managing addition of~~
communicating a session key from a first multicast proxy service node to of a secure
multicast group that includes to a plurality of other multicast proxy service nodes of
the secure multicast group in a communication network, wherein each of the multicast
proxy service nodes is capable of establishing multicast communication and serving as
a key distribution center, the communication system comprising:
a group controller that creates and manages secure multicast communication among
the other multicast proxy service nodes, having a private key;
a computer-readable medium comprising one or more instructions which, when
executed by one or more processors, cause the one or more processors to carry
out the steps of:
creating and storing [[a]] an original group session key associated with the secure
multicast group in a first directory;
authenticating the first multicast proxy service node with a subset of the multicast
proxy service nodes that are affected by an addition of the multicast proxy
service node to the secure multicast group, based on the original group session
key stored in the first directory;
receiving a plurality of private keys from the subset of the multicast proxy service
nodes;
receiving a new group session key for the secure multicast group, for use after addition
of the first multicast proxy service node, from a local multicast proxy service
node that has received the original group session key through periodic
replication of the first directory;
communicating the new group session key private key to the first multicast proxy
event service node; and
communicating a message to the subset of the multicast proxy service nodes that
causes the subset of the multicast proxy service nodes to update their private
keys.

1 [8. (Cancelled)

1 9. (Cancelled)

1 10. (Cancelled)

a¹ 1 13. (Currently Amended) A communication system for creating a secure multicast or
2 broadcast group, the communication system comprising:
3 a plurality of multicast proxy service nodes, each node of the plurality of multicast
4 proxy service nodes having attribute information comprising a group
5 identification value for uniquely identifying a particular one node of the
6 multicast proxy service nodes, ~~wherein the plurality of multicast proxy service~~
7 ~~nodes form a logical arrangement of the multicast proxy service nodes~~
8 ~~according to a tree structure, the tree structure having a root node, intermediate~~
9 ~~nodes, and leaf nodes, one of the multicast proxy service node being designated~~
10 ~~as a primary multicast proxy service node, the primary multicast proxy service~~
11 ~~node being mapped to the root node, the other multicast proxy service nodes~~
12 ~~having private keys corresponding to the group identification values and being~~
13 ~~mapped to the intermediate nodes and the leaf nodes; and~~
14 a directory comprising a directory system agent (DSA) for communicating with one or
15 more of the multicast proxy service nodes to authenticate each of the multicast
16 proxy service nodes and a replication service agent (RSA) for replicating the
17 attribute information of the one or more multicast proxy service nodes; and
18 ~~a plurality of client nodes coupled to one of the multicast proxy service nodes, the one~~
19 ~~multicast proxy service node creating a secure multicast or broadcast client~~
20 ~~group that is separate from the secure multicast or broadcast group;~~
21 wherein one of the multicast proxy service nodes generates a first group session key
22 for establishing the secure multicast or broadcast group among the plurality of
23 multicast proxy service nodes and distributes the first group session key to
24 other multicast proxy service nodes in the secure multicast or broadcast group
25 using directory replication.

1 12. (Cancelled)

1 13. (Currently Amended) A computer-readable medium carrying one or more sequences
2 of instructions for communicating a session key from a first multicast proxy service
3 node of a secure multicast group to a plurality of other multicast proxy service nodes
4 of the secure multicast group in a communication network, wherein each of the
5 multicast proxy service nodes is capable of establishing multicast communication and
6 serving as a key distribution center, wherein execution of the one or more sequences of
7 instructions by one or more processors causes the one or more processors to perform
8 the steps of:

9 creating and storing [[a]] an original group session key associated with the secure
10 multicast group in a first directory;
11 authenticating the first multicast proxy service node with a subset of the multicast
12 proxy service nodes that are affected by an addition of the first multicast proxy
13 service node to the secure multicast group, based on the original group session
14 key stored in the first directory;
15 receiving a plurality of private keys from the subset of the multicast proxy service
16 nodes;
17 receiving a new group session key for the secure multicast group for use after addition
18 of the first multicast proxy service node from a local multicast proxy service
19 node that has received the original group session key through periodic
20 replication of the first directory;
21 communicating the new group session key ~~private key~~ to the first multicast proxy
22 service node; and
23 communicating a message to the subset of the multicast proxy service nodes that
24 causes the subset of the multicast proxy service nodes to update their private
25 keys.

17.
14.

(New) A computer-readable medium as recited in Claim 13, wherein the instructions for authenticating the first multicast proxy service node further comprises instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of authenticating the first multicast proxy service node based on a second directory that comprises a directory system agent (DSA) that communicates with one or more of the multicast proxy service nodes and a replication service agent (RSA) that replicates attribute information of the one or more multicast proxy service nodes.

18.
15.

(New) A computer-readable medium as recited in Claim 13, wherein the instructions for receiving the new group session key further comprises instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of receiving the new group session key from a node of a second directory that comprises a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes and a replication service agent (RSA) for replicating key information of the one or more multicast proxy service nodes.

19.
16.

(New) A computer-readable medium as recited in Claim 13, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of signaling the replication service agent to carry out replication by storing an updated group session key in a local node of the first directory.

20.
17.

(New) A computer-readable medium as recited in Claim 13, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of distributing the original group session key to all nodes by creating and storing the original group session key using a first multicast proxy service node of one domain of the first directory; replicating the first directory; and obtaining the original group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node.

21.
18.

(New) A computer-readable medium as recited in Claim 13, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of distributing the new group session key to all nodes by creating and storing the new group session key using a first multicast proxy service node of one domain of the first directory; replicating the first directory; and obtaining the new group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node.

a1
8.
19.

(New) A communication system as recited in Claim 7, wherein the one or more instructions for authenticating the first multicast proxy service node further comprise one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of:
authenticating the first multicast proxy service node based on a second directory that comprises a directory system agent (DSA) that communicates with one or more of the multicast proxy service nodes and a replication service agent (RSA) that replicates attribute information of the one or more multicast proxy service nodes.

9.
20.

(New) A communication system as recited in Claim 7, wherein the one or more instructions for receiving the new group session key further comprise one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of:
receiving the new group session key from a node of a second directory that comprises a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes and a replication service agent (RSA) for replicating key information of the one or more multicast proxy service nodes.

10.
1 ~~21.~~ (New) A communication system as recited in Claim ~~20~~⁹, further comprising one or
2 more instructions which, when executed by the one or more processors, cause the one
3 or more processors to carry out the step of signaling the replication service agent to
4 carry out replication by storing an updated group session key in a local node of the first
5 directory.

11.
1 ~~22.~~ (New) A communication system as recited in Claim 7, further comprising one or more
2 instructions which, when executed by the one or more processors, cause the one or
3 more processors to carry out the steps of distributing the original group session key to
4 all nodes by creating and storing the original group session key using a first multicast
5 proxy service node of one domain of the first directory; replicating the first directory;
6 and obtaining the original group session key from a local multicast proxy service node
7 that is a replica of the first multicast proxy service node.

12.
1 ~~23.~~ (New) A communication system as recited in Claim 7, further comprising one or more
2 instructions which, when executed by the one or more processors, cause the one or
3 more processors to carry out the step of distributing the new group session key to all
4 nodes by creating and storing the new group session key using a first multicast proxy
5 service node of one domain of the first directory; replicating the first directory; and
6 obtaining the new group session key from a local multicast proxy service node that is a
7 replica of the first multicast proxy service node.

14.
1 ~~24.~~ (New) A communication system as recited in Claim ~~11~~¹³, further comprising:
2 a plurality of client nodes coupled to one of the multicast proxy service nodes, the one
3 multicast proxy service node creating a secure multicast or broadcast client
4 group that is separate from the secure multicast or broadcast group.

15,
25. (New) A communication system as recited in Claim ~~11~~¹³, wherein the plurality of
multicast proxy service nodes form a logical arrangement of the plurality of multicast
proxy service nodes according to a tree structure, the tree structure having a root node,
one or more intermediate nodes, and one or more leaf nodes, one of the multicast
proxy service node nodes being designated as a primary multicast proxy service node,
the primary multicast proxy service node being mapped to the root node, the other
multicast proxy service nodes having private keys corresponding to the group
identification values and being mapped to the one or more intermediate nodes and the
one or more leaf nodes.